CLAIMS

1. (Currently Amended) A method operational for authentication in a public cryptographic system comprising:

creating a first private key and corresponding first public key at a mobile user device;

creating a second private key associated with the first private key and creating a second public key corresponding to the second private key at the mobile user device;

outputting the second private key from the mobile user device such that it is not stored on the mobile user device while retaining the first private key in the mobile user device, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is inaccessible;

transmitting the first public key and the second public key to a verifier device; and

using the retained first private key for authentication of the mobile user device prior to using the second private key.

2. (Previously Presented) The method of claim 1, wherein transmitting the plurality of shares of the second private key comprises:

creating at least two shares of the second private key at the mobile user device; and

wirelessly outputting each share once to a different entity.

3. (Previously Presented) The method of claim 1, further comprising:

re-creating the second private key at one of the mobile user device or a replacement mobile user device using at least some shares of the plurality of shares; and

using the second private key independent of the first private key for authentication of the mobile user device or the replacement mobile user device.

4. (Cancelled)

5. (Previously Presented) The method of claim 3, further comprising:

creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

outputting the third public key to the verifier device.

6. (Previously Presented) The method of claim 5, further comprising:

outputting the third private key once as a plurality of shares such that it can be re-created; and

re-creating the third private key using at least some of the plurality of shares; and

using the third private key for authentication.

7. (Previously Presented) The method of claim 1, wherein the second public and private keys are created independently from the first public and private keys.

8. (Original) The method of claim 3, further comprising:

creating a third private key associated with the second key and creating a third public key corresponding to the third private key;

creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key;

outputting the fourth private key once such that it can be re-created; and

outputting the third and fourth public keys.

9. (Previously Presented) The method of claim 8, further comprising:

disabling use of the second private key for authentication; and

using the third private key for authentication;

re-creating the fourth private key; and

using the fourth private for authentication.

10. (Previously Presented) The method of claim 1, further comprising:

preventing retransmission of the second private key.

11. (Currently Amended) A method for verification in a public cryptographic system comprising:

receiving a first public key from a mobile user device, wherein the first public key has a corresponding first private key stored on the mobile user device;

receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that it is not stored on the mobile user device, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication;

using the first public key for authentication of the mobile user device; and

using the second public key for authentication if the first public key fails.

12. (Previously Presented) The method of claim 11, further comprising:

receiving a third public key from one of the mobile user device or another mobile user device, the third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

13. (Previously Presented) The method of claim 11, further comprising:

receiving a third public key and a fourth public key if the first public key fails and if the second public key results in a successful authentication, wherein the third and the fourth public keys are associated with the second key.

14. (Currently Amended) A mobile user device configured for authentication in a public cryptographic system comprising:

means for creating a first private key and corresponding first public key at the mobile user device;

means for storing the first private key at the mobile user device;

means for creating a second private key associated with the first private key and creating a second public key corresponding to the second private key at the mobile user device;

means for outputting the second private key from the mobile user device such that it is not stored on the mobile user device while retaining the first private key in the mobile user device, wherein outputting the second private key comprises outputting a plurality of shares of the second private key to a plurality of different entities once such that the second private key can be re-created and used when the first private key is inaccessible, wherein the first private key is disabled when the second private key is re-created and used for authentication;

means for outputting the first public key and the second public key to a verifier device; and

means for using the retained first private key for authentication prior to using the second private key.

15. (Previously Presented) The device of claim 14, wherein means for outputting the second private key comprises:

means for creating at least two shares of the second private key at the mobile user device; and

means for outputting each share once to a different entity, wherein subsequent outputting of the second private key is prevented.

16. (Previously Presented) The device of claim 14, further comprising:

means for re-creating the second private key at one of the mobile user device or another mobile user device using at least some shares of the plurality of shares; and

means for using the second private key for authentication of the one of the mobile user device or the other mobile user device.

17. (Previously Presented) The device of claim 16, further comprising:

means for creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

means for outputting the third public key to the verifier device.

18. (Previously Presented) The device of claim 16, further comprising:

means for creating a third private key associated with the second private key and for creating a third public key corresponding to the third private key;

means for creating a fourth private key associated with the third private key and for creating a fourth public key corresponding to the fourth private key;

means for outputting the fourth private key once such that it can be re-created; and

means for outputting the third and fourth public keys to the verifier device.

19. (Currently Amended) A verifier apparatus configured for verification in a public cryptographic system comprising:

means for receiving a first public key from a mobile user device, wherein the first public key has a corresponding first private key stored on the mobile user device;

means for receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that it is not stored on the mobile user device, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication;

means for storing the first public key and the second public key;

means for using the first public key for authentication of the mobile user device; and

means for using the second public key for authentication if the first public key fails.

20. (Previously Presented) The apparatus of claim 19, further comprising:

means for receiving a third public key associated with the second public key from one of the mobile user device or another mobile user device, if the first public key fails and if the second public key results in a successful authentication of the mobile user device or the other mobile user device.

21. (Previously Presented) The apparatus of claim 19, further comprising:

means for receiving a third public key and a fourth public key, if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second public key.

22. (Currently Amended) A non-transitory machine-readable medium comprising instructions for performing a public cryptography, which when executed by a processor causes the processor to:

create a first private key and corresponding first public key;

create a second private key associated with the first private key and create a second public key corresponding to the second private key;

retain the first private key and output the second private key such that it is not stored on a device where the second private key was created, the second private key being output as a plurality of shares to a plurality of different entities once such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication;

output the first public key and the second public key to a verifier device; and

use the retained first private key for authentication prior to using the second private key for authentication.

23. (Previously Presented) The machine-readable medium of claim 22, wherein outputting the second private key further comprises instructions to:

create at least two shares of the second private key; and

output each share once to a different entity.

24. (Previously Presented) The machine-readable medium of claim 22 further comprising instructions to:

recreate the second private key; and

use the second private key for authentication.

25. (Cancelled)

26. (Currently Amended) A non-transitory machine-readable medium comprising instructions for performing a public cryptography at a verifier device, which when executed by a processor causes the processor to:

receive a first public key from a mobile user device, wherein the first public key has a corresponding first private key stored on the mobile user device;

receive a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that it is not stored on a device where the second private key was created, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication;

use the first public key for authentication of the mobile user device; and

use the second public key for authentication if the first public key fails.

27. (Previously Presented) The machine-readable medium of claim 26 further comprising instructions to:

receive a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

28. (Previously Presented) The machine-readable medium of claim 26 further comprising instructions to:

receive a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

29 – 49 (Cancelled)

50. (Currently Amended) A mobile user device used for authentication comprising:

a processor configured to:

generate a first private key and corresponding first public key;

generate a second private key associated with the first private key; and

create a second public key corresponding to the second private key;

a storage medium coupled to the processor, the storage medium configured to store the first private key; and

a transmitter coupled to the processor to:

output the second private key such that it is not stored in the storage medium, the second private key being output as a plurality of shares to a plurality of different entities once, such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication; and

output the first public key and the second public key to a verifier device;

wherein the processor uses the stored first private key for authentication of the mobile user device prior to using the second private key.

51. (Currently Amended) Apparatus used for verification comprising:

a receiver configured to receive a first public key from a mobile user device and to receive a second public key from the mobile user device, wherein the first public key has a corresponding first private key stored on the mobile user device and the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that the second private key is not stored on a device where it was created, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication;

a storage medium coupled to the receiver, configured to store the first and second public keys; and

a processor coupled to the receiver and the storage medium, the processor configured to use the first public key for authentication of the mobile user device, the processor configured to use the second public key for authentication if the first public key fails.

52. (Cancelled)

53. (Previously Presented) The method of claim 1, wherein the second private key is removed from the mobile user device upon transmission of the plurality of shares of the second private key.

54. (Previously Presented) The device of claim 14, wherein the means for outputting the plurality of shares of the second private key comprise means for removing the second private key from the mobile user device.

55. (Previously Presented) The machine-readable medium of claim 22, wherein the processor is further caused to remove the second private key from the mobile device upon outputting the plurality of shares of the second private key to the plurality of different entities.

56. (Previously Presented) The mobile user device of claim 50, wherein the processor is configured to remove the second private key upon the output of the plurality of shares of the second private key to the plurality of different entities.

57. (Currently Amended) A method operational for authentication in a public cryptographic system, comprising:

re-creating a second private key at a mobile user device that has no access to a first private key associated with the second private key, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities;

creating a third private key and a corresponding third public key; ~~and~~

outputting the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at the mobile user device; and

using the second private key for authentication of the mobile user device before using the third private key.

58. (Previously Presented) The method of claim 57, wherein re-creating the second private key at a mobile user device that has no access to the first private key includes re-creating the second private key at a mobile user device different from a mobile user device that created the first private key and the second private key.

59. (Currently Amended) The method of claim 57, ~~further comprising:~~

~~outputting the third private key from the mobile user device while retaining the second private key in the mobile user device,~~ wherein outputting the third private key comprises transmitting a plurality of shares of the third private key from the mobile user device to a plurality of different entities once, such that the third private key can be re-created to replace use of the second private key; and

transmitting the third public key to a verifier device.

60. (Previously Presented) The method of claim 57, further comprising:

creating a fourth private and a corresponding fourth public key;

outputting the fourth private key from the mobile user device while retaining the third private key in the mobile user device, wherein outputting the fourth private key comprises transmitting a plurality of shares of the fourth private key from the mobile user device to a plurality of different entities once, such that the fourth private key can be re-created to replace use of the third private key; and

transmitting the third public key and the fourth public key to a verifier device.

61. (Currently Amended) A mobile user device adapted for authentication in a public cryptographic system, comprising:

means for re-creating a second private key at a mobile user device that has no access to a first private key associated with the second private key, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities;

means for creating a third private key and a corresponding third public key; ~~and~~

means for outputting the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at the mobile user device; and

means for using the second private key for authentication of the mobile user device before using the third private key.

62. (Previously Presented) The mobile user device of claim 61, wherein the means for re-creating a second private key at a mobile user device that has no access to a first private key includes means located at a mobile user device different from a mobile user device that created the first private key and the second private key.

63. (Currently Amended) The mobile user device of claim 61, ~~further comprising:~~

~~means for outputting the third private key from the mobile user device while retaining the second private key in the mobile user device,~~ wherein outputting the third private key comprises

transmitting a plurality of shares of the third private key from the mobile user device to a plurality of different entities once, such that the third private key can be re-created to replace use of the second private key; and

means for transmitting the third public key to a verifier device.

64. (Previously Presented) The mobile device of claim 61, further comprising:

means for creating a fourth private and a corresponding fourth public key;

means for outputting the fourth private key from the mobile user device while retaining the third private key in the mobile user device, wherein outputting the fourth private key comprises transmitting a plurality of shares of the fourth private key from the mobile user device to a plurality of different entities once, such that the fourth private key can be re-created to replace use of the third private key; and

means for transmitting the third public key and the fourth public key to a verifier device.

65. (Currently Amended) A non-transitory machine-readable medium comprising instructions for performing a public cryptography, which when executed by a processor causes the processor to:

re-create a second private key at a mobile user device that has no access to a first private key associated with the second private key, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities;

create a third private key and a corresponding third public key; ~~and~~

output the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at the mobile user device; and

use the second private key for authentication of the mobile user device before using the third private key.

66. (Previously Presented) The machine-readable medium of claim 65, wherein the mobile user device at which the second private key is re-created is a different device from a mobile user device that created the first private key and the second private key.

67. (Currently Amended) The machine-readable medium of claim 65, ~~further comprising instructions to:~~

~~output the third private key from the mobile user device while retaining the second private key in the mobile user device,~~ wherein outputting the third private key comprises transmitting a plurality of shares of the third private key from the mobile user device to a plurality of different entities once, such that the third private key can be re-created to replace use of the second private key; and

further comprising instructions to transmit the third public key to a verifier device.

68. (Previously Presented) The machine-readable medium of claim 65, further comprising instructions to:

create a fourth private and a corresponding fourth public key;

output the fourth private key from the mobile user device while retaining the third private key in the mobile user device, wherein outputting the fourth private key comprises transmitting a plurality of shares of the fourth private key from the mobile user device to a plurality of different entities once, such that the fourth private key can be re-created to replace use of the third private key; and

transmit the third public key and the fourth public key to a verifier device.